CLAIMS

1. A microelectronic apparatus for performing $\underline{\otimes}$ multiplication and squaring in both polynomial based GF(2^q) and GF(p) field arithmetic, squaring and reduction using a serial fed radix 2^{ℓ} multiplier, B, with k character multiplicand segments, A_i, and a k character $\underline{\oplus}$ accumulator wherein reduction to a limited congruence is performed "on the fly", in a systolic manner, with A_i, a multiplicand, times B, a multiplier, over a modulus, N, and a result being at most $2k + 1$ characters long, including the k first emitting disregarded zero characters, which are not saved, where k characters have no less bits than the modulus, the apparatus comprising;

a first (B), and second (N) main memory register means, each register operative to hold at least n bit long operands, respectively operative to store a multiplier value designated B, and a modulus, denoted N, wherein the modulus is smaller than $2^{\mathbf{n}}$;

a digital logic sensing detector, Y_0, operative to anticipate "on the fly" when a modulus value is to be $\underline{\oplus}$ added to the value in the $\underline{\oplus}$ adder accumulator device such that all first k characters emitting from the device are forced to zero;

a modular multiplying device for at least k character input multiplicands, with only one, at least k characters long $\underline{\oplus}$ adder, $\underline{\oplus}$ summation device operative to accept k character multiplicands, the $\underline{\otimes}$ multiplication device operative to switch into the $\underline{\oplus}$ accumulator device, in turn, multiplicand values, and in turn to receive multiplier values from a B register, and an "on the fly" simultaneously generated anticipated value as a multiplier which is operative to force k first emitting zero output characters in the first phase, wherein at each effective machine cycle at least one designated multiplicand is $\underline{\oplus}$ added into the $\underline{\oplus}$ accumulation device;

the multiplicand values to be switched in turn into the $\underline{\oplus}$ accumulation device consisting of one or two of the following three multiplicands, the first multiplicand being an all-zero string value, a second value, being the multiplicand A_i, and a third value, the N_0 segment of the modulus;

an apparatus to anticipate the ℓ bit k character serial input Y_0 multiplier values;

the multiplier values which are input in turn into the multiplying device in the first phase being first the B operand, and concurrently, the second multiplier value consisting of the Y_0, "on the fly" anticipated k character string, to force first emitting zeroes in the output;

an $\underline{\oplus}$ accumulation device, operative to output values simultaneously as multiplicands are $\underline{\oplus}$ added into the $\underline{\oplus}$ accumulation device;

an output transfer mechanism, in the second phase operative to output a final modular $\underline{\otimes}$ multiplication result from the $\underline{\oplus}$ accumulation device.

2. An apparatus as in claim 1 wherein $\underline{\oplus}$ summations into the $\underline{\oplus}$ accumulation device are activated by each new serially loaded higher order multiplier characters.

3. An apparatus as in claim 1, wherein the multiplier characters;

are operative to cause no $\underline{\oplus}$ summation into the $\underline{\oplus}$ accumulation device if both the input B character and the corresponding input Y_0 character are zeroes;

are operative to $\underline{\oplus}$ add in only the A_i multiplicand if the input B character is a one and the corresponding Y_0 character is a zero;

are operative to $\underline{\oplus}$ add in only the N, modulus, if the B character is a zero, and the corresponding Y_0 character is a one; and

are operative to $\underline{\oplus}$ add in the $\underline{\oplus}$ summation of the modulus, N, with the multiplicand A_i if both the B input character and the corresponding Y_0 character are ones.

4. An apparatus as in claim 1, operative to preload multiplicand values A_i and N, into two designated preload buffers, and to $\underline{\oplus}$ summate these values into a third multiplicand preload buffer, obviating the necessity of $\underline{\oplus}$ adding in each multiplicand value separately.

5. An apparatus as in claim 1, wherein the multiplier values are serial single character in input and the output of the $\underline{\oplus}$ accumulation device is serial single character output, wherein the Y_0 detect device is operative to anticipate only one character in a clocked turn.

6. An apparatus as in claim 1, wherein the $\underline{\oplus}$ accumulation device performs modulo 2, XOR addition/subtraction, wherein all carry bits in addition and subtraction components are disregarded, thereby precluding provisions for overflow and further limiting convergence in computations.

7. A $\underline{\otimes}$ multiplication apparatus as in claim 1 wherein all carry inputs are disabled to zero, denoted, $\mathcal{S}$=0, typically operative to perform polynomial based multiplication.

8. An apparatus as in claim 1 wherein an $\mathcal{S}$ equal to zero acting on an element in a circuit equation computing in GF(2^q), the $\mathcal{S}$ designates omitted circuitry and all adders and subtractors, designated $\underline{\oplus}$ have been reduced to XOR, modulo 2 addition/subtraction elements.

9. An apparatus as in claim 1 wherein k first emitting zeroes will egress from the device controlled by the following four quantities in anticipating the next in turn Y_0 character:

i. the ℓ bit S_{out} bits of the result of the ℓ bit by ℓ bit mod 2^{ℓ} $\underline{\otimes}$ multiplication of the right-hand character of the A_i register times the B_d character of the B Stream, $A_0 \cdot B_d \bmod 2^{\ell}$;

ii. the first emitting carry out character from the $\underline{\oplus}$ accumulation device, $\mathcal{S}(CO_0)$;

iii. the ℓ bit S_{out} character from the second from the right character emitting cell of the $\underline{\oplus}$ accumulation device, SO_1;

iv. the ℓ bit J_0 value, which is the negative multiplicative inverse of the right-hand character in the N_0 modulus multiplicand register.

wherein values, $A_0 \cdot B_d \bmod 2^{\ell}$, $\mathcal{S}(CO_0)$, and SO_1 are $\underline{\oplus}$ added character to character together and "on the fly" multiplied by the J_0 character to output a valid Y_0 zero-forcing anticipatory character to force an ℓ bit egressing string of zeroes.

10. An apparatus as in claim 1, wherein $\underline{\otimes}$ multiplication on polynomial based operands is performed in a reverse mode, multiplying from right hand MS characters to left hand LS characters, operative to perform modular reduced $\underline{\otimes}$ multiplication without Montgomery type parasitic functions.

11. An apparatus as in claim 1 where the preload buffers are serially fed and where multiplicand values are preloaded into the preload buffers on the fly from a multiplicity of memory devices.

12. An apparatus as in claim 1, wherein a previous value, emitting from an additional n bit register, S, is $\underline{\oplus}$ summated into the output value of the $\underline{\oplus}$ accumulation device via an ℓ bit $\underline{\oplus}$ adder circuit such that first emitting output characters are zeroes when the Y_0 detector is operative to detect the necessity of $\underline{\oplus}$ adding moduli to the $\underline{\oplus}$ summation in the $\underline{\oplus}$ accumulation device, wherein the Y_0 detector is operative to detect utilizing the next in turn $\underline{\oplus}$ added characters $A_0 \cdot B_d \bmod 2^{\ell}$, $\mathcal{S}(CO_0)$, SO_1, S_d and $\mathcal{S}(CO_z)$, the composite of $\underline{\oplus}$ added characters to be finite field $\underline{\otimes}$ multiplied on the fly by the ℓ bit J_0 value, where $\underline{\oplus}$ defines the addition and $\underline{\otimes}$ defines the multiplication as befits the finite field used in the process.

13. An apparatus as in claim 1, wherein for $\ell = 1$, J_0 is implicitly 1, and the J_0 $\underline{\otimes}$ multiplication is implicit, without additional hardware.

14. An apparatus as in claim 1 wherein a comparator is operative to sense a finite field output from the $\underline{\otimes}$ modular multiplication device, working in GF(p), where the first right hand emitting k zero characters are disregarded, where the output is larger than the modulus, N, thereby operative to control a modular reduction whence said value is output from the memory register to which the output stream from the multiplier device is destined, and thereby precluding allotting a second memory storage device for the smaller product values.

15. A device as in claim 1 wherein for $\underline{\otimes}$ modular multiplication in the GF(2^q), the apparatus is operative to multiply without an externally precomputed more than ℓ bit zero-forcing factor.

16. A method according to claim 1 operative to compute a J_0 constant by resetting either the A operand value or the B operand value to zero and setting the partial result value, S_0, to 1.

17. A microelectronic apparatus for performing interleaved finite field $\underline{\otimes}$ modular multiplication of integers A and B operative to generate an output stream of A times B modulus N wherein n the number of characters in the modulus operand register is larger than k, wherein the $\underline{\otimes}$ multiplication process is performed in iterations, wherein at each interleaved iteration with operands input into a $\underline{\otimes}$ multiplying device, consisting of N, the modulus, B, a multiplier, a previously computed partial result, S, and a k character string segment of A, a multiplicand, the segments progressing from the A_0 string segment to the A_{m-1} string segment, wherein each iterative result is $\underline{\oplus}$ summated into a next in turn S, temporary result, in turn, wherein first emitting characters of iterative results are zeroes, the apparatus comprising:

first (B), second (S) and third (N) main memory registers, each register capable of storing and outputting operands, respectively operative to store a multiplier value, a partial result value and a modulus, also denoted N;

a modular multiplying device operative to $\underline{\oplus}$ summate into the $\underline{\oplus}$ accumulation device, in turn one or two of a plurality of multiplicand values, in turn, during the phases of the iterative $\underline{\otimes}$ multiplication process, and in turn to receive as multipliers, in turn, inputs from a first value B register, second, from an "on the fly" anticipating value, Y_0, as a multiplier to force first emitting right-hand zero output characters in each iteration, and third values from the modulus, N, register;

the multiplicand parallel registers operative at least to receive in turn, values from the A, B, and N register sources, and in turn, also a multiplicand zero forcing Y_0, value;

a first emitting zero forcing Y_0 detect device operative to generate a binary string operative to be a multiplier during the first phase and operative to be a multiplicand in the second phase;

multiplicand values to be switched into the accumulation device for the first phase consisting of a first zero value, a second value, A_i, which is a k character string segment of a multiplicand, A, and a third value N_0, being the first emitting k characters of the modulus, N;

a temporary result value, S, resulting from a previous iteration, operative to be summated with the value emanating from the accumulation device, to generate a partial result for the next in turn iteration;

multiplicand values to be input, in turn, into the accumulation device for the second phase being, a first zero value, a second A_i operand, remaining in place from the first phase, and a third Y_0 value having been anticipated in the first phase;

multiplier values input into the multiplying device in the first phase being a first emitting string, B_0, being the first emitting string segment of the B operand, concurrently multiplying with the second multiplier value consisting of the anticipated Y_0 string which is simultaneously loaded character by character as it is generated into a preload multiplicand buffer for the second phase;

the two multiplier values input into the apparatus during the second phase being the left hand n - k character values from the B operand, designated $\underline{B}$, and the left hand n - k characters of the N modulus, designated $\underline{N}$, respectively; and

a multiplying flush out device operative in the last phase to transfer the left hand segment of a result value remaining in the accumulation device into a result register.

18. An apparatus as in claim 17, wherein multiplication on polynomial based operands is performed in a reverse mode, multiplying from MS characters to LS characters, operative to perform modular reduction without Montgomery type parasitic functions.

19. An apparatus operative to anticipate the Y_0 value using first emitting values of the multiplicand, and present inputs of the B multiplier, carry out values from

the accumulation device, summation values from the accumulation device, the present values from the previously computed partial result, and carry out values from the adder which summates the result from the accumulation device with the previous partial result.

20. An apparatus as in claim 19 wherein k first emitting zeroes will egress from the device controlled by the following six quantities in anticipating the next in turn Y_0 character:

i. the ℓ bit S_{out} bits of the result of the ℓ bit by ℓ bit mod 2^{ℓ} multiplication of the right-hand character of the A_i register times the B_d character of the B Stream, $A_0 \cdot B_d$ mod 2^{ℓ};

ii. the first emitting carry out character from the accumulation device, $\mathcal{S}(CO_0)$;

iii. the ℓ bit S_{out} character from the second from the right-hand character emitting cell of the accumulation device, SO_1;

iv. the next in turn character value from the S stream, S_d;

v. the ℓ bit carry out character from the Z output full adder, $\mathcal{S}(CO_z)$;

vi. the ℓ bit J_0 value, which is the negative multiplicative inverse of the right-hand character in the N_0 modulus multiplicand register;

wherein values, $A_0 \cdot B_d$ mod 2^{ℓ}, $\mathcal{S}(CO_0)$, SO_1, S_d are added character to character together and "on the fly" multiplied by the J_0 character to output a valid Y_0 zero-forcing anticipatory character to force an ℓ bit egressing character string of zeroes.

21. An apparatus as in claim 17 comprised of at least one sensor operative to compare the output result to N, the modulus, the mechanism operative to actuate a second subtractor on the output of the result register, thereby to output a modular reduced value which is limited congruent to the output result value precluding the necessity to allot a second memory storage for a smaller result.

22. An apparatus as in claim 17 where a value which is a summation of two multiplicands is loaded into a preload character buffer with at least a *k* characters memory means register concurrently whilst one of the values is loaded into a preload buffer.

23. An apparatus with only one accumulation device, and an anticipating zero forcing mechanism operative to perform a series of interleaved modular multiplications and squarings concurrently performing the equivalent of three natural integer multiplication operations, such that a result is an exponentiation.

24. An apparatus as in claim 17 where next in turn used multiplicands are preloaded into preload register buffer means on the fly.

25. An apparatus as in claim 17 where a value which is a summation of two multiplicands is summated into at least a *k* character register concurrently whilst one of the values is loaded into its preload buffer.

26. An apparatus as in claim 17 wherein apparatus buffers and registers are operative to be loaded with values from external memory sources and said buffers and registers are operative to be unloaded into the external memory source during computations, such that the maximum size of the operands is dependent on available memory means.

27. An apparatus as in claim 17 wherein memory register means are typically serial single character in/serial single character out, parallel at least *k* characters in/parallel at least *k* characters out, serial single character in/parallel at least *k* characters out, and parallel *k* characters in/serial single character out.

28. An apparatus as in claim 17 wherein the final phase of a multiplication type iteration, the multiplier inputs are zero characters operative to flush out the left hand segment of the carry save accumulator memory.

29. An apparatus as in claim 17 where next in turn used multiplicands are preloaded into preload memory buffers on the fly.

30. An apparatus as in claim 17 where multiplicand values are preloaded into the preload buffers on the fly from central storage memory means.